Multinational Experiment 7
Outcome 3 – Cyber Domain
Objective 3.3

Guidelines for Decision Makers

Version 2.0

03 October 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Multinational Experiment 7 Outcome 3 - Cyber Domain Objective 3.3 Guidelines for Decision Makers Version 2.0 03 October 2012	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
The aim of MNE7 Objective 3.3 is to improve partners' and coalition members' understanding of the current legal frameworks applicable to the cyber domain in order to better handle cyber incidents, while providing decision makers with the appropriate tools for decision-making andm options for response. Guidelines for Decision Makers - Legal Analysis for Cyber Incidents (GDMs) are envisaged as the MNE7 Obj. 3.3 solution to provide the Decision Makers' legal advisors and Subject-matter Experts (SMEs), primarily at the political and the strategic level, with a practical instrument to a. pin down, in a coherent framework, the main elements and features of a given cyber incident b. support the analysis conducted by legal experts through an international legal perspective c. identify the legal threshold crossed by a cyber incident in terms of violation of the international law d. recommend, through the legal assessment process and the dialogue among legal experts,lawful options for response.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**25**	

Table of contents

This document was prepared by obj.3.3 legal working group, led by the following team: Prof. Talitha Vassalli di Dachenhausen , Naples University "Federico II", RADM (ret) Pio Forlani, Dr. Rita Mazza, Dr. Annachiara Rotondo, Dr. Claudia Pirillo, and supported by IAI (Istituto Affari Internazionali/ International Affairs Institute). Life Management and Configuration Control over this document, generated by a cooperative effort under MNE 7 umbrella, will be established by the Italian Defence General Staff-Centre for Defence Innovation.

FOREWORD

Multinational Experiment 7 (MNE7) is a two-year multinational and interagency Concept Development and Experimentation (CD&E) effort aimed to improve coalition capabilities to ensure access to and use of the global commons domain (air, maritime, space and cyber) through application of the comprehensive approach.

AIM and SCOPE

The aim of MNE7 Objective 3.3 is to improve partners' and coalition members' understanding of the current legal frameworks applicable to the cyber domain in order to better handle cyber incidents, while providing decision makers with the appropriate tools for decision-making and options for response.
Guidelines for Decision Makers - Legal Analysis for Cyber Incidents (GDMs) are envisaged as the MNE7 Obj. 3.3 solution to provide the Decision Makers' legal advisors and Subject-matter Experts (SMEs), primarily at the political and the strategic level, with a practical instrument to:

a. pin down, in a coherent framework, the main elements and features of a given cyber incident;

b. support the analysis conducted by legal experts through an international legal perspective;

c. identify the legal threshold crossed by a cyber incident in terms of violation of the international law;

d. recommend, through the legal assessment process and the dialogue among legal experts, lawful options for response.

A. GUIDELINES STARTING POINT: THE ANALYTICAL MODEL FOR LEGAL ANALYSIS OF CYBER INCIDENTS

The fundamental aim of the GDMs is represented by the Analytical Model for cyber incident legal analysis depicted in the matrix below. This offers a template (see Briefing Template for Cyber Incident Legal Assessment at Appendix B) for the conduct of legal analysis (see also Concept Framework para. C3).

The matrix has been divided into seven main columns (in green), designed to lead legal analysis towards the main elements of a cyber incident to be taken into account from a legal perspective.

Within the analytical model framework, a given cyber incident can be described by highlighting the characterizing seven key elements in the appropriate boxes along every column.

More than one box may be highlighted to describe the combination of multiple features of the same element (e.g. a cyber attack carried out through privately owned nodes and public nodes at the same time, or consequences on multiple aspects).

Subsequently, the legal analysis of the given cyber incident may be conducted, column by column, by linking each element (column) and feature (highlighted boxes) to the facets of international legal framework which apply, through identification of the international obligation that has been breached.

It is important to emphasise that the mutual influence among the elements of the analytical model, as well as the possible interactions among relevant features, will also be taken into account to avoid too mechanistic an approach to the legal analysis.

B. INTERACTIONS AMONG TOPICS (COLUMNS OF ANALYTICAL MODEL) FOR IDENTIFICATION OF LEGAL THRESHOLDS

Analytical Model Matrix

<table>
<tr><th>Context</th><th>Actor</th><th>Assessment of activities</th><th>Source</th><th>Target/ Objectives</th><th>Consequences</th><th>Extent</th><th>Breach of an international obligation</th><th colspan="2">Legal Thresholds</th></tr>
<tr><td>Peace time</td><td>State</td><td>Cyber Attack
- disruptive
- destructive</td><td>State</td><td>State</td><td>Non material</td><td>Small</td><td></td><td colspan="2">Domestic Issue</td></tr>
<tr><td>Crisis</td><td>Person/Entity</td><td>Cyber Defence</td><td>Military</td><td>Military</td><td>Economic</td><td>Mild</td><td>Sovereignty. Non interference on internal affairs of a State.
Human rights: Freedom of Expression</td><td colspan="2">Wrongful Act</td></tr>
<tr><td>Armed Conflict</td><td>Terrorist</td><td>Cyber Exploitation</td><td>Private</td><td>Private</td><td>Physical Damage</td><td>Large</td><td rowspan="3">Prohibition of use of force and threat.
Humanitarian law</td><td rowspan="2">International Crime</td><td>Terrorism</td></tr>
<tr><td></td><td>Undetermined</td><td>Undetermined</td><td>Undetermined</td><td>Critical Infrastructure</td><td>OPSEC</td><td></td><td>Crime of Aggression</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Civilian Infrastructure</td><td>Casualties</td><td></td><td colspan="2">Armed Attack</td></tr>
</table>

1. Context
   The Context is the status of the international relations between the relevant actors involved in the cyber incident (i.e. peacetime, crisis, armed conflict). It is recognized that there will almost certainly be a blurring across these categories in the future, as we face becoming involved in increasingly complex and wicked problems.

Context	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
Peacetime	Traditional sphere of International Law			
Crisis				
Armed Conflict	IHL / LOAC	Additional Protocol I to the Geneva Conventions of 12 August 1949, 8 June 1977		Situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, are not armed conflicts (Article 1(2) of Additional Protocol II to the Geneva Conventions of 12 August 1949, 8 June 1977).

Definition of "peacetime": The expression identifies the relationship among States that are not involved in an armed conflict. In international relations, peacetime is not only the absence of war or violent conflict, but also the presence of positive and respectful cultural and economic relationships.

Definition of "crisis": Whilst there is no overarching agreed definition of the term "crisis" in international law., a crisis could be defined as a "highly intensive phase of a problematic development which is directly threatening the existence or the social interaction of people and cannot be overcome with usual means and which, as a forced challenge, leaves open a positive or negative outcome"[1].

Through consideration of AP II Article 1(2), a "crisis" may include any disturbance or tension within a State, such as riots, isolated and sporadic acts of violence and other acts of a similar nature. Domestic crises may have many possible sources, including natural disasters. In this

[1] Taken from an Austrian Concept on Civil- Military Cooperation.

context they may be designated as “national crises” and States may have domestic laws and regulations dealing with those situations.

Definition of “international crisis”: An international crisis can be defined as the deterioration of the political situation and the rising tension in a State or a region, which constitutes a threat to international peace and security (UN SC Resolutions since 1992).

Definition of International Armed Conflict (IAC): An IAC occurs when one or more States have recourse to armed force against another State, regardless of the reasons or the intensity of this confrontation. No formal declaration of war or recognition of the situation is required.
Common Article 2 to the Geneva Conventions of 1949 states that:
"In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.
The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance."

Definition of Non International Armed Conflict (NIAC): A NIAC can be defined as being between governmental forces and non-governmental armed groups, or between such groups only. IHL treaty law also establishes a distinction between non-international armed conflicts in the meaning of Common Article 3 of the Geneva Conventions of 1949 and non-international armed conflicts falling within the definition provided in Article 1 of Additional Protocol II.

It should be noted that situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, do not amount to a NIAC – the situation must reach a certain level of confrontation and intensity.

2. Actor

States and International Organisations, which are subjects of the international community, whether acting in that capacity or through their recognised organs, can be regarded as one classification of Actors. However, a cyber incident may originate from individuals or a group whose responsibility in international law is only possible if their activity is attributable to the State[2], or to an International Organisation (according to its constituting treaty). The problem of attribution is arguably the key element to be investigated and carefully analysed in order to address the appropriate response within the international legal framework. The situation is markedly different for individuals acting as terrorists, whose responsibility under international law may be recognized under International Legal Sources.[3]

Actor	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
State	Montevideo Convention	Article 1, Montevideo Convention on the Rights and Duties of States		
Terrorist	United Nations GA	Adapted from UN GA Resolution 49/60 Declaration on Measures to Eliminate International Terrorism		NB. There is no agreed definition of terrorism in international law
Person/ Entity	Various	Various, including UDHR, ECHR, Rome Statute etc.		
Undeter-mined				

Definition of "State": States are the prime subjects in international law, and State sovereignty within its territory is a fundamental principle. All the States share the features of having a geographic territory, a permanent population and a government which exercises effective and independent control over that territory. Article 1 of the Montevideo Convention on the Rights and Duties of States, which can be viewed as an accurate statement of customary international law, states that:

"The state as a person of international law should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other states."

[2] Article 2b (Elements of an internationally wrongful act of a State) International Law Commission (ILC) Draft Articles on State's Responsibility (see also the Concept Framework para B.2.1)

[3] Concept Framework, para B. 2. 1 under Treaties

Definition of "Terrorist": Whilst international law lacks a universal definition of "terrorist", individual States may have a definition in their national legislation. One such definition could be seen as an individual or group engaged in criminal acts intended or calculated to provoke a state of terror in the general public, a group or person or persons for political purposes.
However, the various sectorial counter-terrorism conventions define and criminalize particular categories of terrorist activities, providing an indirect definition of "terrorist":
Article 2.1 of the 1997 International Convention for the Suppression of Terrorist Bombings indirectly defines a terrorist as:
"Any person [that] unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place or public use, a State or government facility, a public transportation system or an infrastructure facility:
a) With the intent to cause death or serious bodily injury; or
b) With the intent to cause extensive destruction of such a place, facility or system, where such a destruction results in or is likely to result in major economic loss."
Article 19 expressly excluded from the scope of the convention certain activities of State Armed Forces and of self-determination movements.

Article 2.1 of the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention) indirectly defines a terrorist as "any person" who "by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an act "intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

The 2005 United Nations International Convention for the Suppression of Acts of Nuclear Terrorism provides at Art.2
"1. Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally:
(a) Possesses radioactive material or makes or possesses a device:
  (i) With the intent to cause death or serious bodily injury; or
  (ii) With the intent to cause substantial damage to property or to the environment;
(b) Uses in any way radioactive material or a device, or uses or damages a nuclear facility in a manner which releases or risks the release of radioactive material:
  (i) With the intent to cause death or serious bodily injury; or
  (ii) With the intent to cause substantial damage to property or to the environment; or
  (iii) With the intent to compel a natural or legal person, an international organization or a State to do or refrain from doing an act".

In the context of the EU, the most important documents have been the Common Position 2001/931/CFSP of 27 December 200115 and the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.
These documents set out a series of measures but, more importantly, they are the first documents providing solid criteria for the definition of terrorists and terrorist groups.

According to these definitions there are three basic criteria to be employed in order to characterize a group or an act as terrorist:
a) ***The acts:*** Both the Common Position and the Council Decision refer to a series of criminal acts that will be deemed as terrorist offences
b) ***The aim:*** According to both the Common position and the Council Decision, the above acts, in order to constitute terrorist offences, must be committed with the intention of (i) seriously intimidating a population, (ii) compelling a government or international organization to perform or abstain from performing any act or (iii) seriously destabilizing or destroying the fundamental political, constitutional or social structures of a state or international organization.
c) ***Participation in a terrorist organization:*** The 2001 Common Position lists offences relating to the participation in a terrorist group among the acts considered as terrorist. On the

contrary, the 2002 Council Decision creates a separate category of offences for direction of or participation in a terrorist group or financing such activities and obliges member states to introduce separate legislation for the punishment of such activity.

Whereas the 2001 Common Position does not make any kind of distinction between the groups that would perform terrorist acts, the 2002 Framework Decision, at para. 11 of its preamble, specifically states *"... actions by the armed forces of a State in the exercise of their official duties are not governed by this Framework Decision"*, thus following the idea that the notion of terrorism should be confined to the activities of private groups and cannot, under any circumstances, include actions by State organs or official State policies, even if they match the abovementioned criteria.

Definition of "Person/entity": An individual or group of individuals, that may be liable to personal responsibility under international law and/or entitled to non-derogable rights under international human rights law.

3. Assessment of Activities
Information in cyberspace can be used, manipulated, influenced or exploited. This may result in either desired or unintentional effects, through cyber attacks and cyber exploitation or in order to provide cyber defence.

Assessment of activities	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
Cyber Attack - disruptive - destructive	United Nations Charter	Use of Force, Art.2.4 Threat to the peace, breach of peace or act of aggression, Art.39 Armed Attack, Art.51		
Cyber Defence				Cyber Defence should not be equated with the term “self defence”, which can be a legitimate and lawful response to an Armed Attack, since cyber defence also embraces preventive measures
Cyber Exploitation	National Criminal Law	N/A		
Undetermined				

Definition of “Cyber Attack”: Hostile actions taken in cyberspace to modify, disrupt, deny, degrade or destroy information or functionality (MNE7 Outcome 3 working definitions), or “ any action taken to undermine the functions of a computer network for a political or national security purpose”. By using an effects-based approach, a cyber-incident can be qualified as armed force or an armed attack if it causes a destructive effect comparable to that of conventional weapons.

Definition of “Cyber Defence”: The application of protective measures to prevent cyber threats and mitigate the impact of cyber incidents (MNE7 Outcome 3 Working Definition) and the employment of military capabilities, strategies and coordination to achieve cyber security.
From a legal perspective, cyber defence can be regarded as a range of activities taken by a State, ranging from preventive measures in order to achieve cyber security, to an active defensive response performed by a State to counter a threat of or hostile activity performed by another State or individual or non-State actors.

However, the expression "cyber defence" should not be equated with the term “self defence” which is an inherent right in response to an armed attack (UN Charter, article 51), since cyber defence also embraces preventive measures.
The use of the word ”defence” can also be interpreted either as a strict reference to military measures, or as all measures, proactive as well as reactive, taken by a State to defend and protect its digital infrastructure. In this context, the definition only refers to military defence.

Definition of “Cyber exploitation”: Cyber exploitation refers to operations conducted through the use of computer networks in order to gather data from target information systems and networks. They are operations performed with the purpose of gathering technical or intelligence information, in order to enable and carry out operations conducted by other computer networks. It can be viewed as intelligence activity, or even as activity carried out in preparation for a cyber attack.

From a legal perspective, in peacetime this kind of activity can arguably be regarded as criminal activity. Cyber exploitation, depending on whether it is intrusive or not, may be regarded as either perfectly legitimate and lawful Open Source Intelligence (OSINT), or as intelligence activity (i.e. espionage) or criminal activity (e.g. digital intrusion), depending on any applicable national criminal law. In the case of criminal activity, with the exception of defensive measures, it would normally be the responsibility for national police forces to investigate and stop such action.

4. Source
In the event of a cyber incident, it is imperative that effective legal analysis (from the perspective of international law) is conducted in order to identify the origin of the source cyber node (e.g. government, military or private).

Source	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
State			Column 2	
Military			Column 2	
Private				
Undeter-mined				

Definition of State source: is one attributable to a State actor as defined above.

Definition of Military source: is one attributable to any organised armed forces, groups or units which are under a command responsible towards a government or authority for the conduct of its subordinates.

Definition of Private source: is any source which is attributable to a specific actor which is neither State nor military.

5. Target/Objectives
   The target/objectives of a cyber incident may be in the layers of the State, military or private domain. Within these layers, possible consequences affecting critical infrastructures and civilian infrastructures are of particular relevance, due to, for example, threats to a population's vital security deriving from significant damage caused by a cyber incident.

Target / Objectives	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
State	Additional Protocol I to Geneva Conventions, Art. 54, 56		Column 4	
Military	Additional Protocol I to Geneva Conventions, Art. 52		Column 4	
Private	Additional Protocol I to Geneva Conventions, Art. 48, 52, 54, 56, 57		Column 4	
Critical Infrastructure*				
Civilian Infrastructure*				

***Critical and / or Civilian Infrastructure can be a target that will affect either the State, the Military or the Private arena, or combinations thereto.**

Definition of "Critical Infrastructure": There are many definitions of critical infrastructure; consequently, it can be described through different formats of reports, directives, strategies and law.
NATO has defined critical infrastructure as facilities and services that are vital to the basic operations of a given society.[4]
The European Programme for Critical Infrastructure Protection (EPCIP) has created a European Critical Infrastructure list, based on input from the EU Member States (MSs). A European Critical Infrastructure is one so designated because it is considered of the highest importance for the Community and which, if disrupted or destroyed would affect two or more MSs, or a single Member State if the critical infrastructure is located in another Member State. This

[4] 162 CDS 07 E rev 1 – The Protection of Critical Infrastructures (2007).

includes trans-boundary effects resulting from interdependencies between inter-connected infrastructures across various sectors.
EPCIP has also issued Council Directive 2008/114/EC on the identification of European Critical Infrastructures, which includes an assessment of the need to improve their protection. The Directive, which is oriented towards a definition of critical infrastructure of a single Member State, states in article 2 (a):
""Critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".

Definition of "Civilian Infrastructure": The method of defining civilian infrastructure is dependant upon the legal situation and whether it is in peacetime or in a state of armed conflict.

In peacetime, the difference between civilian and military infrastructure lies in the premise that most States prefer not to use its military forces for civilian purposes, thus there are special laws regulating military activity in peacetime. At its simplest, it can be regarded that all infrastructures are civilian and that military infrastructure is an exception from that general rule. Military infrastructure would be easiest defined in peacetime by ownership; if it is owned and operated by the military, it should be regarded as military infrastructure.

In a situation of armed conflict or war, the legal definition of civilian infrastructure is based in the application of international humanitarian law, due to the obligation to observe the principle of distinction. This rule states that war is to be waged against the enemy´s armed forces and not against its civilian population. This principle originates from the preamble of the St Petersburg Declaration, which states:
"The only legitimate object which states should endeavour to accomplish during war is to weaken the military forces of the enemy".
This principle is further expressed in Additional Protocol I (1977) to the Geneva Conventions of 1949, which states, at Article 48:
"In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives".[5]

[5] See, in particular, AP1, Part IV, and AP2, Part IV.

6. Consequences

The consequences resulting from a cyber incident, as with other categories of incidents, could range from casualties (human losses), physical damage, non material effects (e.g. psychological impact, economic impact, etc), and, particularly in the military field, issues with Operational Security (OPSEC).

Consequences	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
Non material	Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001	Compensation Art. 36, 38 Satisfaction Art. 37	Strictly linked to Column 7	Arts 30 (Cessation and non-repetition), 39 (Contribution to the injury), 49 (Object and limit of countermeasures); Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001
Economic Damage	Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001	Compensation Art. 36, 38 Satisfaction Art. 37	Strictly linked to Column 7	Arts 30 (Cessation and non-repetition), 39 (Contribution to the injury), 49 (Object and limit of countermeasures); Draft Articles on Responsibility of States for Internationally Wrongful Acts
Physical Damage	Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001	Compensation Art. 36, 38 Satisfaction Art. 37	Strictly linked to Column 7	Arts 30 (Cessation and non-repetition), 39 (Contribution to the injury), 49 (Object and limit of countermeasures); Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001

OPSEC	Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001	Compensation Art. 36, 38	Strictly linked to Column 7	Arts 30 (Cessation and non-repetition), 39 (Contribution to the injury), 49 (Object and limit of countermeasures); Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001
Casualties	Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001	Compensation Art. 36 Satisfaction Art. 37	Strictly linked to Column 7	Arts. 30 (cessation and non-repetition), 39 (Contribution to the injury), 49 (Object and limit of countermeasures); Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001

7. Extent

The extent of consequences from a cyber incident may be unverifiable from a technical perspective, but the perceived (provable) level of the extent could be a relevant factor in an (international legal) analysis, aimed at providing assessments regarding legal options for response as well as the correct determination of the caused damage. In the case of countermeasures as a response, the extent of the consequences from a cyber incident is a key element in order to ensure the proportionality of the countermeasure itself.[6]

Extent	Legal Framework of Reference	Legal references	Links to other Features of the analytical model	Special Notes
Small			Strictly Linked to Column 6	
Mild			Strictly Linked to Column 6	
Large			Strictly Linked to Column 6	

[6] Article 51 of International Law Commission (ILC) Draft Articles on State's Responsibility.

8. Breach of an International Obligation and Legal Thresholds

The final outcome of the legal analysis process will be achieved through the elements in the last two columns (in blue). The identified breach of an international obligation, as a result of guided analysis across the eight green columns, will drive the assessment of the related legal threshold. Should the cyber incident be identified as a domestic issue, (internal) Response Options will have to be selected within the applicable domestic Legal Framework. If the cyber incident is identified as being of an international nature (wrongful act, international crime, armed attack) possible response options (available to the Decision Maker, depending upon his level of authority) will also have to be assessed against the international legal framework.

It is important to underline again that mutual influence between the elements of the analytical model, as well as possible interactions among the relevant features, should be taken into account to avoid any mechanistic approach to the legal analysis.

As a result, the last column of the matrix (Legal Thresholds) represents the output of the legal analysis conducted along the first eight columns, taking into consideration the legal framework, the legal references and the rules associated with every feature of the given cyber incident.

A description of thresholds, within an international law framework, into which a given cyber incident may fall (see also Concept Framework B.2.1) is provided below:

Internationally Wrongful Act of a State

An internationally wrongful act of a State occurs when conduct consisting of an action or omission is attributable to the State under international law and constitutes a breach of an international obligation of the State.[7]

International Crime

Whilst there is some debate over what crimes can be regarded “international crimes”, the term generally refers to acts and omissions which have been criminalised under international law (in accordance with the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts). According to the Rome Statute of the International Criminal Court (ICC), the Court’s jurisdiction “shall be limited to the most serious crimes of concern to the international community as a whole”: that is, the crime of genocide, crimes against humanity, war crimes and the crime of aggression (see below).

The distinction between a wrongful act and international crime has to be assessed in every given cyber incident and depends on the kind of international rule that has been violated. The violation of international customary or conventional rule is a wrongful act, whereas, according to Part 2 Chapter III of the International Law Commission (ILC) Draft Articles on State’s Responsibility, serious breaches of an international obligation under peremptory norms of general international law are international crimes, whose particular consequences are ruled in article 41 of the same chapter. Peremptory norms of general international law (the so called *Jus Cogens*) are defined in article 53 of Vienna Convention on the Law of treaties as “… a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character”. The said distinction is fundamental in an international legal analysis aimed to provide assessment regarding legal options for response, in view of the *erga omnes* effect of international crimes (like terrorism, aggression, armed conflict and so on) under article 41 para 2 of International Law Commission (ILC) Draft Articles on State’s Responsibility, according to which “no State shall recognize as lawful a situation created by a serious breach within the meaning of article 40, nor render aid or assistance in maintaining that situation”.

[7] Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001 Article 2.

Crime of aggression
The Rome Statute of the International Criminal Court refers to the crime of aggression as one of the "most serious crimes of concern to the international community", and provides that the crime falls within the jurisdiction of the International Criminal Court (ICC). A definition of this crime was agreed upon by Parties to the Rome Statute in 2010 through RC/Res 6 of 11 June 2010.

Terrorism
No single, universally accepted legal definition of "terrorism" currently exists. Member States of the United Nations have agreed upon several "sectorial" Treaties against terrorism, such as the International Convention for the Suppression of Terrorist Bombings, which define some specific types of acts that States Parties are bound to criminalise. These acts can therefore be considered "terrorism" under international law, at least with regard to the States Parties to each particular treaty (for reference to other treaties see CF B.2.1 under treaties on terrorism). Additional Protocols I and II to the Geneva Conventions stipulate that during an armed conflict, "acts or threats of violence the primary purpose of which is to spread terror among the civilian population" are prohibited.

Armed Attack
Article 2(4) of the Charter of the United Nations stipulates that UN Members must "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state". Under Article 51, States are, however, entitled to resort to armed force in self-defence against an "armed attack".
There is no definition of what constitutes an armed attack in the Charter. In fact, "Armed attack" is, although closely related, a narrower category than "threat or use of force". The GA Resolution no.3314/74 (XXIX) on the definition of aggression (which is now the content of art. 8 bis par. 2 of Rome Statute of the ICC according to the resolution RC/RES.6 , 11 June 2010) trying to link art.2(4), and art.51 of the UN Charter clarifies that the only aggression justifying self-defence is an armed one. In the *Nicaragua* case, the ICJ, also failing to define "armed attack", expressly affirmed that the use of force could be divided into two categories, "most grave" (those constituting armed attacks) and "less grave", giving the word "force" at art 2 (4) a broader meaning than art. 51.

9. Response Matrix

The response matrix (at the following page) represents the last stage of the cyber incident analysis process depicted by the analytical model. This matrix has been re-arranged starting from an original source (*JP-5 August 2011, Appendixes E and F).*

For every possible threshold a given cyber incident may cross, a set of associated possible (**although not exhaustive**) response options may be associated. As soon as a threshold is identified through the legal analysis process, a set of legal options for response, within the international law framework, shall be highlighted in green.

Response options whose legal viability remains questionable and subject to alternative interpretations shall be highlighted in yellow.

Response options which are clearly forbidden, under the circumstances of the identified legal threshold, shall be highlighted in red.

Legal Thresholds		**Options for Response**			
Domestic Law Issue		Internal Response Options based on Domestic Legal Frameworks			
Wrongful Act		Gain support through the United Nations.	Alert and introduce special teams (e.g., public diplomacy).	Identify the steps to peaceful resolution.	Take actions to gain support of allies and friends.
		Increase cultural group pressure.	Reduce international diplomatic ties.	Reduce security assistance programs.	Ensure consistency of strategic communication messages.
		Enact restrictions on technology transfer.	Enact restrictions on technology transfer.	Encourage national and international financial institutions to restrict or terminate financial transactions.	Encourage national and international financial institutions to restrict or terminate financial transactions.
		Protect friendly communications systems and ISR assets (computer network defence, operations security, information assurance).	Publicize violations of international law.	Maintain an open dialogue with the news media.	Take steps to increase national public support.
		Freeze or seize real property where possible.	Freeze or seize real property where possible.	Freeze or seize real property where possible.	Declare diplomatic personnel as “persona(e) non grata”
		Make public declarations of non-proliferation policy.	Impose sanctions on communications systems and intelligence, surveillance, and reconnaissance (ISR) technology transfer.	Initiate non-combatant evacuation procedures.	Increase informational efforts.
		Increase communication systems and ISR processing and transmission capability.	Restrict activities of diplomatic missions.	Prepare to withdraw or withdraw embassy personnel.	Embargo goods and services.
		Increase defence support to public diplomacy.	Increase information operations.	Demonstrate international resolve.	Enact trade sanctions.
		Publicize increased force presence, joint exercises, military capability	Upgrade alert status.	Restrict travel of national citizens.	Increase intelligence, surveillance, and reconnaissance.
		Influence adversary decision makers (political, military, and social).	Increase training and exercise activities	Initiate or increase show-of-force actions.	Increase active and passive protection measures.
		Implement meaconing, interference, jamming, and intrusion of adversary informational assets.	Increase information measures directed at the opponent's military forces.	Initiate the installation of a United Nation Sanction Committee	Interrupt satellite downlink transmissions.
Interna-tional Crime	**Armed Attack**	Individual or collective self-defence	Report to the United Nations Security Council	Deploy forces into or near the potential operational area	
	Other Crimes	Initiate or increase the cooperation with the ICC	Increase international cooperation of law enforcement agencies		

APPENDIX A

1.Check list for legal analysis supported by the Cyber Incident Analytical Model (CIAM):

In a context of
☐ PEACE
☐ ARMED CONFLICT
☐ CRISIS
...a
☐ STATE ACTOR
☑ PERSON/ENTITY
☐ TERRORIST
☐ UNDETERMINABLE ACTOR
...makes/
☐ CYBER ATTACK
☐ CYBER EXPLOITATION
☐ CYBER DEFENSE
☐ UNDETERMINABLE CYBER ACTIVITY
...that configures a
☐ BREACH OF INTERNATIONAL OBLIGATION
☑ BREACH OF A NATIONAL OBLIGATION
...from a
☐ PUBLIC SOURCE
☐ MILITARY SOURCE
☐ PRIVATE SOURCE
☐ UNDETERMINABLE SOURCE
...which determines
☐ IMMATERIAL DAMAGE
☐ ECONOMIC DAMAGE
☐ PHYSICAL DAMAGE
☐ HUMAN LOSSES
☐ OPSEC
☐ NO DAMAGE
...that have
☐ SMALL
☐ MILD
☐ LARGE
...consequences.

NOTE: If both green boxes are selected, the legal framework for the cyber incident will be based on national domestic legislation and NOT international law.

APPENDIX B

BRIEFING TEMPLATE FOR CYBER INCIDENTS LEGAL ASSESSMENT
(FOR EXCLUSIVE USE BY LEGAL ADVISORS).

Brief description of the cyber incident (condense the contents of the incident report and the incident classification suggested by the incident Reporter):

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Classification of the main elements and features of the cyber incident i.a.w. Cyber Incident Analytical Model (CIAM);

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Legal assessment of the cyber incident (see the blue columns of the CIAM):

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Options recommended (Response Matrix to be used as a guidance):

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....